

Analyse der Performance Parameter eines ZigBee-Funknetzes

Prof. Dr.-Ing. Tobias Felhauer

Badstr. 24
77652 Offenburg
Tel. 0781 205-208
E-Mail: felhauer@fh-offenburg.de

1965: Geboren
Studium der Elektrotechnik/Nachrichtentechnik
an der Universität Kaiserslautern

1990: Diplom

1990–1994: wissenschaftlicher Mitarbeiter am Lehrstuhl für hochfrequente Signalverarbeitung der Universität Kaiserslautern

1994: Promotion über neuartige Verfahren zur hochgenauen Vermessung von Funkkanälen mit Bandspreizsignalformen

1994–1999: Labor- und Projektleiter im Zentralbereich Technik der DaimlerChrysler Aerospace AG, Ulm

1994: Literaturpreis der ITG für eine Veröffentlichung in IEEE AES.

1997: Best Paper Award des amerikanischen Institutes of Navigation (ION)

seit 1999: Professor an der Hochschule Offenburg für das Fachgebiet Telekommunikationstechnik, Leiter des Labors Telekommunikationstechnik

seit 2000: Mitglied des Instituts für Angewandte Forschung (IAF) der Hochschule Offenburg

Forschungsschwerpunkte: Digitale Funkkommunikation und Satellitennavigation



IV.4 Analyse der Performance Parameter eines ZigBee-Funknetzes

Prof. Dr. Tobias Felhauer

Im Rahmen dieses Projekts wurde im Labor Telekommunikationstechnik der Hochschule Offenburg ein flexibel konfigurierbares Funknetz nach dem ZigBee-Standard aufgebaut. Mit Hilfe diverser Messgeräte und Analyse-Tools wurden die wesentlichen Performance Parameter dieses Funknetzes unter realen Betriebsbedingungen evaluiert. So wurden z. B. Erkenntnisse über die Empfängerempfindlichkeit, die effektiv erreichbare Datenrate sowie das Interferenzpotential gewonnen, die Voraussetzungen für die optimale Nutzung dieser neuen Funktechnologie sind.

ZigBee ist eine neue WPAN (Wireless Personal Area Network) – Funktechnologie zur Vernetzung von einfachen Geräten und Sensoren. Genauer betrachtet sind die nachrichtentechnischen Aspekte der physikalischen Schicht und der Medienzugriffsschicht im Standard IEEE 802.15.4 spezifiziert, auf dem die höheren Protokollschichten des eigentlichen ZigBee-Standards aufbauen. Ihren Namen hat diese unkomplizierte, an einfachste Endgeräte gerichtete Funktechnologie von der Zick-Zick-Tanzkommunikation der Honigbiene, die – richtig interpretiert – den Artgenossen die Richtung, Qualität und Entfernung zu einer Futterquelle anzeigt. Anwendungsbereiche der ZigBee-Technologie liegen vor allem in der Sensorik, Gebäudeautomation und Medizintechnik, wo Netzwerke mit einfachsten Endgeräten zum Einsatz kommen, die weder hohe Bandbreite/Datenrate noch komplexe Netz-

architekturen benötigen, aber hohe Ansprüche an die Latenzzeit beim Verbindungsaufbau und an eine geringe Leistungsaufnahme für lange Batterielebenszeiten stellen. Hierin diversifiziert sich die ZigBee-Technologie z. B. von der etablierten Bluetooth-Technologie, die schwerpunktmäßig Applikationen mit mittlerer und hoher Übertragungsrate im PC-Bereich und bei der Vernetzung von z. B. Mobiltelefonen und PDAs adressiert.

In einem ZigBee-Netzwerk findet man prinzipiell zwei Gerätetypen unterschiedlicher Komplexität: RFDs (Reduced Function Devices) und FFDs (Full Function Devices). Ein FFD hat die Möglichkeit, mit RFDs oder mit anderen FFDs zu kommunizieren, während ein RFD nur mit einem FFD interagieren kann. Ein FFD tritt innerhalb des PANs (Personal Area Network) als Koordinator, Router oder als komplexes Endgerät auf, wohingegen ein RFD auf die Rolle eines Endgerätes geringerer Komplexität beschränkt ist.

Mit RFDs und FFDs können nach Abb. IV.4-1 PANs sowohl mit Stern als auch mit Peer-to-Peer Topologien aufgebaut werden. Die Stern Topologie definiert einen zentralen Koordinator, über den jegliche Kommunikation im PAN abgewickelt wird. Peer-to-Peer Netze beinhalten ebenfalls einen Koordinator, erlauben jedoch zusätzlich eine Kommunikation zwischen den übrigen FFDs, welche nicht die Rolle des Koordinators übernommen haben. Dadurch können komplexere Topologien wie eine Baumstruktur oder ein vermaschtes Netzwerk durch den Einsatz von Routern (FFDs) geschaffen werden.

Für die ZigBee-Kommunikation können drei lizenzfreie Frequenzbereiche unter Beachtung regionaler Einschränkungen genutzt werden. Im global frei verfügbaren und deshalb von den meisten Endgeräten verwendeten 2,4GHz-ISM-Band sind nach IEEE802.15.4 16 Kanäle im Abstand von 5MHz definiert, in denen jeweils ZigBee-Datensignale mit einer Datenrate von 250kbit/s übertragen

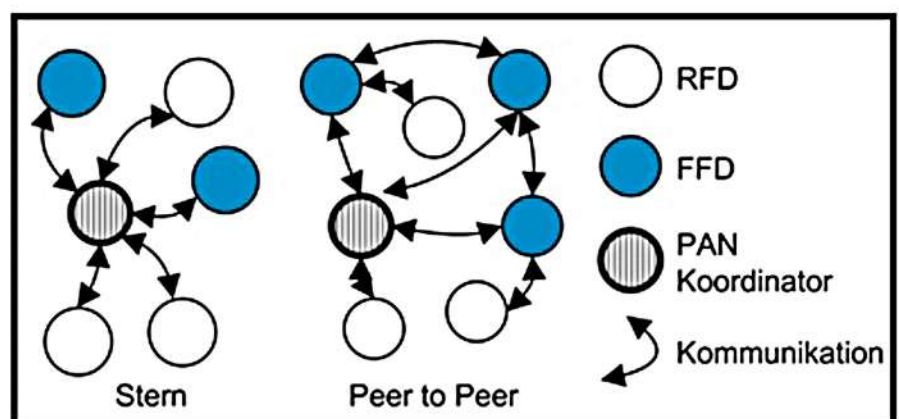


Abb. IV.4-1: Netztopologien in einem ZigBee PAN

werden können. Um den Betrieb auch bei hoher Auslastung zu sichern, sind zusätzlich lizenzfreie Frequenzbereiche zwischen 868–868,6 MHz mit einem 20kBits/s Kanal in Europa sowie 10 weitere 40kBits/s Kanäle bei 902–928 MHz zur Nutzung in den USA vorgesehen.

Um einen Frequenzdiversitäts-Gewinn und eine höhere Störresistenz zu erzielen, wird bei ZigBee die Bandspreizmodulation DS-SS (Direct Sequence Spread Spectrum) eingesetzt. Dazu werden in der 2,4 GHz-Variante jeweils 4 zu übertragende Bits zu einer Bitkombination (Symbol) zusammengefasst. Den 16 möglichen Bitkombinationen werden dann gemäß eines Look-up-Table Spreizcodes bestehend aus 32 chips zugeordnet. Diese Spreizcodes werden schließlich im Rahmen der Bandspreizmodulation durch eine OQPSK-Modulation auf den Träger des verwendeten Frequenzkanals moduliert. Daraus ergibt sich ein resultierender Spreizfaktor von 8 (4Bit → 32chips) bzw. bei einer Nutzbitrate von 250kbit/s eine resultierende Chiprate von 2 Mchips/s.

Im Gegensatz zur PHY-Schicht, welche lediglich einen universellen Rahmentyp kennt, spezifiziert IEEE 802.15.4 mit Data-, Beacon-, Command- und ACK-Frames insgesamt vier verschiedene Frames auf MAC Ebene. Von besonderer Bedeutung für die Synchronisation von Endgeräten und für den Kanalzugriff ist dabei der Beacon-Frame. Um sich an die Anforderungen verschiedenster Applikationen flexibel anpassen zu können, sind bei ZigBee zwei Netzwerkmodi mit unterschiedlichen Kanalzugriffsmechanismen möglich. Im einfachen Non-Beacon-Enabled-Network-Modus erfolgt der Kanalzugriff der Stationen durch einen lokal ablaufenden unslotted CSMA/CA-Algorithmus asynchron, d.h. ohne Bindung an zeitliche Rahmenbedingungen. Hat eine Station gerade keine Daten zu versenden, wechselt sie in einen Energiesparmodus und schaltet ihren Transceiver ab. Dieser Modus erlaubt keine Bevorzugung bestimmter Stationen durch Vergabe reservierter Zeitschlitze. Im komplexeren Beacon-Enabled-Network-Modus synchronisiert der PAN-Koordinator die Kanalzugriffe der von ihm verwalteten Stationen durch das periodische Versenden von Beacon-Frames. Die Zeitdauer zwischen zwei Beacons (Beacon Intervall) unterteilt

sich nach Abb. IV.4-2 in eine aktive Phase, in der die Kommunikation der Teilnehmer untereinander stattfindet, und in eine inaktive Phase, in der die Stationen in einen Energiesparmodus wechseln. Sowohl die Beacon-Intervall-Dauer als auch die Dauer der aktiven und inaktiven Phase können vom PAN-Koordinator frei konfiguriert werden. Die Konfigurationsparameter werden dabei als Parameter innerhalb des Beacon-Frames den verwalteten Stationen mitgeteilt. Durch diese flexible Konfigurationsmöglichkeit ist die Anpassung an verschiedenste Anforderungen möglich. In unkritischen Sensoranwendungen können lange Energiesparphasen mit gelegentlichen Datenübertragungen realisiert werden, wohingegen bei kommunikationsintensiven Applikationen mehr Wert auf Übertragungszeit und Datendurchsatz, als auf Energiesparsamkeit gelegt wird. Die Flexibilität wird weiter dadurch erhöht, dass die aktive Phase in 16 gleichgroße Zeitschlitze unterteilt wird, von denen je nach Bedarf vom PAN-Koordinator maximal 7 Zeitschlitze einer wettbewerbsfreien Phase CFP (Contention Free Period) zur Realisierung von Quality of Service und die restlichen Zeitschlitze einer Wettbewerbsphase CAP (Contention Access Period) zugeordnet werden können, in denen

die Stationen als Wettbewerber gemäß dem slotted CSMA/CA-Mechanismus um den Kanalzugriff konkurrieren. Zeitschlitze innerhalb der wettbewerbsfreien Phase werden als GTS (Guaranteed Timeslots) bezeichnet und müssen von den Stationen explizit beim Koordinator angefordert und reserviert werden. Dabei kann ein ZigBee-Modul auch mehrere GTS beanspruchen.

Einige wesentliche technische Charakteristika der ZigBee-Technologie sind in Tab. IV.4-1 nochmals zusammenfassend aufgelistet.

Im Rahmen dieses Projekts wurde zur Analyse der Performance Parameter eines ZigBee-Netzwerkes mit Modulen des ZDK2420 Development Kits der Firma Chipcon ein entsprechendes Funknetz aufgebaut und konfiguriert. Dieses Funknetz besteht nach Abb. IV.4-3 aus einem ZDK2420 Evaluation Board (EV), das für Datenratenmessungen, Transmitter Tests und für diverse Protokollanalysen verwendet wird, sowie aus weiteren sechs ZDK2420 Development Boards (DB), die sowohl als FFD als auch als RFD im Funknetz agieren können. Für die Analyse der HF-Parameter der ZigBee-Signale wurde ein Spektrumanalysator Anritzu MS2665C eingesetzt.

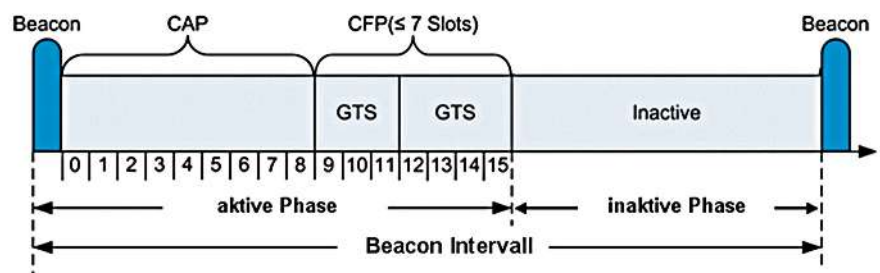


Abb. IV.4-2: Strukturierung des Kanalzugriffs im Beacon-Enabled-Network-Modus

| | | | |
|------------------|-------------------------------------|----------------------|-------------------------------|
| Gerätetypen | RFD; FFD | | |
| Basistopologien | Stern; Peer-to-Peer | | |
| Frequenzbereiche | 868-868,6 MHz (Europe) | 902-928 MHz (USA) | 2400-2483,5 MHz (weltweit) |
| Kanalanzahl | 1 | 10 | 16 |
| Modulationsart | DBPSK/DS-SS | DBPSK/DS-SS | OQPSK/DS-SS |
| Datenrate | 20 kbit/s | 40 kbit/s | 250 kbit/s |
| Reichweite | max. 75 m | | |
| Betriebsmodi | Non Beacon Enabled / Beacon Enabled | | |

Tab. IV.4-1: Wesentliche technische Parameter einer ZigBee-Kommunikationsverbindung

Weiterhin wurden folgende von der Firma Chipcon zur Verfügung gestellte vier Software-Tools verwendet:

- Z-Trace: dient zur Kontrolle der Eingabe über das User-Interface der Development Boards.
- RF-Studio: dient zur Konfiguration der in allen ZigBee-Modulen verwendeten Chipcon CC2420 Transceiverchips.
- AVR-Studio: wird zur Programmierung der ATMEGA128 Mikroprozessoren der Development Boards benötigt.
- Daintree Sensor Network Analyser: Dieses Sniffer-Tool ermöglicht diverse Protokollanalysen im betrachteten ZigBee-Funknetz.

In dem zuvor beschriebenen ZigBee-Funknetz wurden unter Nutzung der oben aufgelisteten Tools umfangreiche Analysen durchgeführt, um wichtige Performance Parameter dieser neuen Funktechnologie im realen Betrieb zu ermitteln. Einige exemplarische Analyseergebnisse werden nachfolgend aufgeführt.

Abb. IV.4-4 zeigt zunächst das Leistungsdichtespektrum eines ZigBee-Signals mit der Mittenfrequenz 2405 MHz und der Chiprate 2 Mchip/s. Da im Rahmen der Bandspreiztechnik eine OQPSK-Modulation mit Halbsinus-Grundimpulsfilter verwendet wird, berechnet sich mit der Chipperiode T_{chip} der Energie eines Chips E_{chip} und der Trägerfrequenz $f_{Träger}$ das Leistungsdichtespektrum theoretisch zu

$$\Phi(f)/dB = 10 \cdot \log$$

$$\left(E_{chip} \cdot \frac{\cos(2\pi(f - f_{Träger})T_{chip})}{1 - 16 \cdot (f - f_{Träger})^2 \cdot T_{chip}^2} \right)$$

Die von diesem theoretischen Leistungsdichtespektrum ermittelbaren Werte für die Null-zu-Null Bandbreite der Hauptkeule von 3 MHz und des Pegel der ersten bzw. zweiten Nebenmaxima von 23,5 bzw. 30,8 dB unterhalb des Pegels des Hauptmaximums können durch Analyse des in Abb. IV.4-4 dargestellten Messergebnisses sehr gut bestätigt werden. Weitergehende messtechnische Analysen haben gezeigt, dass trotz Halbsinus-Grundimpulsfilterung über die Nebenmaxima des Leistungsdichtespek-

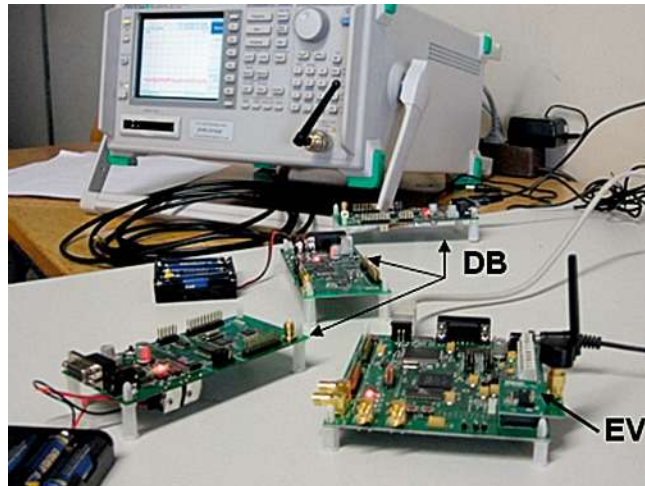


Abb. IV.4-3: ZigBee-Funknetz basierend auf Chipcons ZDK2420 Development Kit

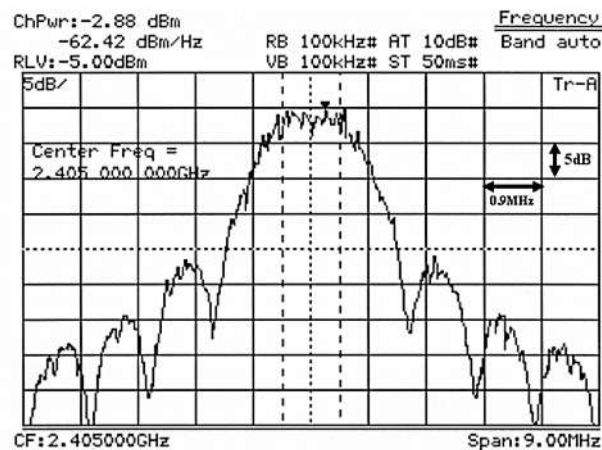


Abb. IV.4-4: Leistungsdichtespektrum

trums auch bei Berücksichtigung der Empfangsfiltercharakteristik insbesondere bei örtlich eng benachbarten ZigBee-Modulen signifikante Nachbarkanalinterferenzen auftreten können, die den Kanalzugriff erschweren und damit die effektive Datenrate vermindern.

Gemäß dem Standard IEEE 802.15.4 darf bei einer Empfängergrenzeempfindlichkeit von $P_{min} = -85dBm$ eine maximale Paketfehlerrate von $PER_{max} = 1\%$ nicht überschritten werden. Diese Empfängerempfindlichkeit wurde evaluiert, indem jeweils 1000 ZigBee-Datenpakete mit unterschiedlicher Sendeleistung übertragen wurden und im Empfänger die Paketfehlerrate PER abhängig von der Empfangsleistung P bestimmt wurde. Die in Abb. IV.4-5 dargestellten Messergebnisse zeigen, dass bis zu einer Empfangsleistung von $-90dBm$ keine Paketfehler auftreten; bei einer weiteren Verringerung der Empfangsleistung steigt die Paketfehlerrate jedoch sehr stark an.

Die theoretisch maximale Bruttodatenrate auf der Funkschnittstelle ist in Tab. IV.4-1 für ZigBee-Module im 2,4GHz-ISM-Band zu 250kbit/s angegeben. Dieser Wert für die effektive Datenrate wird jedoch im realen Funkbetrieb niemals erreichbar sein, da zum einen der Protokolloverhead sowie diverse Verzögerungszeiten durch z. B. den Backoff-Algorithmus im CSMA-CA-Zugriffsmechanismus oder die Aktivierung und Deaktivierung der Transceiver auftreten. Zur Evaluierung der in einem realen ZigBee-Funknetz tatsächlich erreichbaren Datenrate wurden Funknetze bestehend aus unterschiedlich vielen ZigBee-Modulen konfiguriert und jeweils die Zeitdauer gemessen, die zum erfolgreichen Senden von 10000 Datenpaketen mit jeweils 102 Byte MAC-Payload benötigt wird. Auf der Basis dieser gemessenen Zeitdauern wurde dann die Bruttodatenrate (inkl. Protokolloverhead) und Nettodatenrate (exkl. Protokolloverhead) sowohl für ein einzelnes

ZigBee-Modul als auch für das gesamte Funknetz bestimmt. Die Ergebnisse dieser Analyse sind in Abb. IV.4-6 dargestellt. Man erkennt, dass die maximale mittlere Datenrate eines ZigBee-Moduls mit zunehmender Anzahl der Module im Funknetz tendenziell abnimmt, bedingt im Wesentlichen durch die zunehmende Konkurrenzsituation beim Kanalzugriff im Rahmen des CSMA/CA-Mechanismus. Betrachtet man die Datenrate des gesamten Funknetzes, d.h. aller ZigBee-Module im betrachteten Funknetz, so bleibt diese bereits ab zwei Modulen in guter Näherung konstant. Betrachtet man die Werte in Abb. IV.4-6, so erkennt man, dass die Datenrate einzelner ZigBee-Module stets deutlich unterhalb der theoretisch maximalen Datenrate von 250kbit/s liegt. Diese theoretisch maximale Datenrate würde nur erreicht werden, wenn ein Modul ununterbrochen und ohne jeglichen Protokolloverhead senden würde, was in einem realen Funknetz niemals möglich ist.

Die im Rahmen dieses Projekts bisher gewonnenen Erkenntnisse wurden nach entsprechender didaktischer Aufbereitung inzwischen in eine entsprechende Laborübung integriert, um Studenten die Möglichkeiten zu bieten, Erfahrungen mit der neuen Funktechnologie ZigBee zu erlangen.

Der Autor dankt allen, die zum Gelingen dieses Projekts beigetragen haben – besonderer Dank gebührt dabei Herrn Tim Benneckenstein.

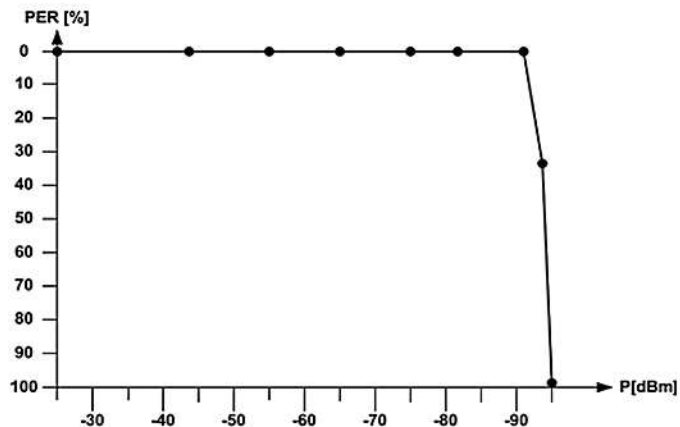


Abb. IV.4-5: Paketfehlerrate PER abhängig von der Empfangsleistung P

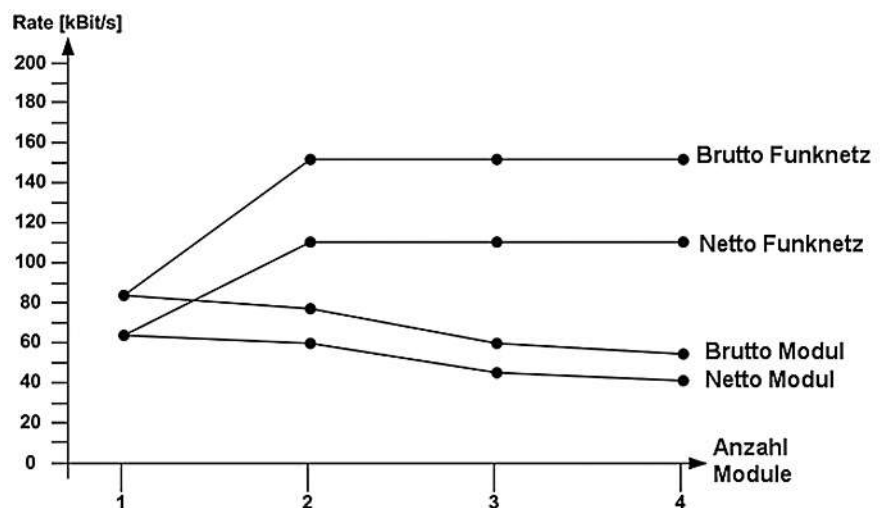


Abb. IV.4-6: Effektive Datenraten unter verschiedenen Bedingungen